REMARKS

Claims 32-55 were examined, and all were rejected. Claims 32, 42-44, and 50-55 have been amended to more distinctly claim subject matter which the applicants regard as the invention. No new matter has been introduced into the application by these amendments. Claims 32-55 remain pending.

Claim Rejections - 35 USC § 102

Claims 32-33, 35-41, 44, 46-49, and 53-55

Claims 32-33, 35-41, 44, 46-49, and 53-55 stand rejected under 35 USC § 102(e) as being allegedly anticipated by Wessman (US Patent 7,111,005 B1). The rejection is traversed with regard to the claims as now presented.

It is well settled that a reference must teach every element or aspect of a claim in order to be considered prior art under 35 USC § 102(e). Wessman fails to do so.

Independent claims 32, 44, 53, and 55 recite an appliance for protecting data stored in a web server environment that does not secure data received from the web before it is stored, comprising a processor for securing and/or unsecuring data which is stored in and/or retrieved from a database by a web server environment. The appliance provides the securing/unsecuring function independently from the data storage/retrieval function performed by the web server environment.

In contrast, Wessman describes a server that provides both securing/unsecuring data and storing/retrieving the data, wherein the securing/securing functions are provided in conjunction with, and cannot be separated from, the storing/retrieving functions. For example, Wessman, claim 1, recites "receiving a request at the database system to store data in the database system; wherein the request is directed to one or more columns of the database system that have been designated as encrypted..." The examiner cites Wessman as providing a web server environment that does not secure data received from the web before it is stored. That is incorrect. A search of Wessman reveals that Wessman does not contain even a single instance of

- 11 -

any of the terms "web," "www," "http," or any other term indicating the presence of a web

server. Therefore, Wessman does not disclose a web server environment as recited in the claims.

Furthermore, in Wessman data is encrypted because the column of the database in which it is to

be stored is designated as an encrypted column. Therefore, even if Wessman did disclose a web

server environment that stores data, it could not be a web server environment that "does not

secure ... data ... before it is stored," as recited in the claims.

Wessman is further cited for identifying sensitive data contained in a data transaction.

That is also incorrect. In Wessman, the data itself is not even examined. Instead, the "[d]atabase

server **112** examines metadata **222** to determine if the column where the data will be stored is

encrypted." Thus, in Wessman data is not encrypted because it is identified as being sensitive, as

claimed. Rather, data is encrypted because the associated metadata indicates that it is to be

stored in an encrypted database column, without regard for whether or not the data itself is

sensitive. Both sensitive and non-sensitive data would be encrypted before being stored in the

column designated as encrypted. Moreover, since data is identified for encryption because the

database column where it is to be stored is designated as encrypted, the identification function is

inextricably linked to the data storage function.

In contrast, in the claims as currently presented, sensitive data is identified and encrypted

before being forwarded to the web server environment for storage. The encryption function is

disassociated from the storage function, and the identified sensitive data is encrypted regardless

of where it is stored. Indeed, the sensitive data need not even be stored in columns of a database

at all, but might, for example, be stored in a flat file. In addition, the database need not natively

support encryption.

The claims present several advantages over Wessman. The claimed appliance transforms

data of a network transaction by encryption/decryption, and re-inserts the transformed data back

into the same network transaction that was present before the encryption/decryption took place.

Because the claimed appliance isolates the encryption/decryption function from the

storage/retrieval function, it can be inserted between two components, such as a client and a

database server that does not support encryption functionality, without modifying the database server component to support encryption.

That has value in legacy web server environments comprising database server components that do not support encryption. Furthermore, because the claimed appliance operates independently of the database layer, it can be used to encrypt data in more than one type of database, regardless of whether each database type has native support for encryption. The appliance can also ensure uniformity of encryption across heterogeneous database environments. Wessman cannot provide any of those capabilities. Separating the encryption from the database server as claimed further enhances the security of the solution, because neither the clear-text data nor the encryption keys appear on the database server machine. This prevents system users from being able to use memory snooping or similar techniques on the database server to defeat the encryption mechanism. Database servers are generally susceptible to such a threat, particularly in the "rogue database administrator" scenario, wherein an insider with high database privilege is ordinarily able to gain access to the sensitive data.

At least for the reasons presented above, Wessman does not disclose or suggest all of the features claimed, and claims 32, 44, 53, and 55 are allowable over Wessman. Claims 33 and 35-41 depend from claim 32, claims 46-49 depend from claim 44, and claim 54 depends from claim 53, and those claims comprise all of the features of their respective base claims. Therefore, without prejudice to their own individual merits, those claims are also allowable over Wessman for at least the same reasons as their base claims.

Reconsideration and withdrawal of the section 102 rejection of claims 32-33, 35-41, 44, 46-49, and 53-55 are respectfully requested.

Claims 43 and 51

Claims 43 and 51 stand rejected under 35 USC § 102(e) as being allegedly anticipated by Rollins (US Patent 7,415,429 B2). The rejection is traversed with regard to the claims as now presented.

- 13 -

Claims 43 and 51 recite a transparent encryption (TE) appliance for protecting a web server environment against tampering at the client by securing cookies provided by the web server environment. As described at p. 13, ll. 7-17, in the prior art "there is no mechanism for ensuring that users do not maliciously modify cookies while they reside on the user's machine. The TE Appliance can be used to overcome this problem..." As claimed, a cookie is provided by the web server environment, and is secured by the encryption appliance and provided to a client computer without providing means to the client to unsecure the cookie.

In contrast, Rollins describes a so-called integrated order mechanism (IOM) that facilitates commercial transactions between a client, a merchant web server, and a so-called wallet server for storing client information useful in a commercial transactions. Although Rollins discloses the use and protection of various cookies in conjunction with the IOM, it is not clear exactly what is protected, or how and where the protection is implemented. In particular, the merchant web server **306** can send a cookie to the IOM containing order information (Rollins, col. 14, l. 66 through col. 15, l. 3), and the IOM can generate cookies and send them to the client (Rollins, col. 18, ll. 13-16). Further, "in the situation where client information is stored in a wallet cookie on client **703** or IOM **708**, an encrypted wallet cookie may be used to protect the client information;" (Rollins, col. 20, ll. 14-16). However, there is no disclosure of the IOM providing for encryption/decryption of unencrypted cookies provided by the merchant web server and/or the wallet server. Furthermore, in Rollins the reason for encrypting a cookie is to protect the client information contained therein, and not to prevent the client from maliciously hacking the cookie and compromising the web server environment. In Rollins, the information in the cookie can be used at the client to pre-fill an online form. In order to do so, means to decrypt the cookie must be provided to the client.

At least because Rollins does not disclose or suggest an appliance for receiving a cookie provided by a separate web server environment, securing the cookie against tampering at the client, without providing means to the client to unsecure the cookie as claimed, claims 43 and 51 are allowable over Rollins.

Reconsideration and withdrawal of the section 102 rejection of claims 43 and 51 are respectfully requested.

Claim Rejections - 35 USC § 103

Claims 34, 42, 45, and 50

Claims 34, 42, 45, and 50 stand rejected under 35 USC § 103(a) as being allegedly unpatentable over Wessman in view of Rollins. The rejection is traversed in view of the claims as now presented.

Claims 34 and 42 depend from claim 32, and claims 45 and 50 depend from claim 44, and it is noted that Rollins is relied on only for the additional features of claims 34, 42, 45, and 50. However, Rollins does not supplement Wessman to provide all of the features of claims 32 and 44 missing therefrom, as discussed above. Therefore, combining Wessman and Rollins as suggested by the examiner does not result in the claims, nor does the combination render the claims obvious. Therefore, the section 103 rejection of claims 34, 42, 45, and 50 is not supported and, without prejudice to their own individual merits, they are allowable over the cited references for at least some of the same reasons their respective base claims are allowable over Wessman alone.

Reconsideration and withdrawal of the section 103 rejection of claims 34, 42, 45, and 50 are respectfully requested.

Claims 52

Claim 52 stands rejected under 35 USC § 103(a) as being allegedly unpatentable over Wessman in view of Johnson (US 6,898,577 B1). The rejection is traversed in view of the claims as now presented.

The examiner cites Wessman for protecting sensitive data stored in a web server environment, comprising a web server environment that stores data received from the web and does not secure the data before it is stored, and a transparent encryption appliance comprising a processor for securing and/or unsecuring data, in the manner recited in claim 32. For the reasons presented above in connection with the section 102 rejection of claim 32, Wessman does not in fact provide all of the features of claim 52 contended by the examiner to be found therein. Johnson is relied on for disclosing the sensitive data as a password, and verifying the secured

- 15 -

password to authenticate an action requiring authorization. However, Johnson does not supplement Wessman to provide all of the features of claim 52 missing therefrom. In particular, Wessman in view of Johnson, whether individually or in any possible combination, do not disclose, suggest, or render obvious at least a web server environment that stores data received from the web and does not secure the received data before it is stored, or a transparent encryption appliance comprising a processor that identifies a password contained in a data transaction, secures the password, replaces in the data transaction the identified password with the secured password, and provides the data transaction with secured password to the web server environment. Therefore, the section 103 rejection of claim 52 in view of Wessman combined with Johnson is not supported, and claim 52 is allowable over those references.

Reconsideration and withdrawal of the section 103 rejection of claim 52 are respectfully requested.

Conclusion

In view of the foregoing amendment and remarks, applicants respectfully submit that the present application, including claims 32-55, is in condition for allowance and an early notice of allowance is respectfully requested.

Respectfully submitted,

DAN BONEH, *et al.*

BY:

ROBERT E. CANNUSCIO
Registration No. 36,469
DRINKER BIDDLE & REATH LLP
One Logan Square
18th and Cherry Streets
Philadelphia, PA 19103-6996
Tel: 215-988-3309
Fax: 215-988-2757
Attorney for Applicant

PHIP/ 758351.1